REMARKS

The Office Action has been carefully reviewed, and the following remarks herein are considered responsive thereto. Claims 1–12 are currently pending in this application. Claims 1–12 have been amended by this amendment. New dependent claims 13–33 have been added.

It is noted that no claim 7 was presented in the claims as filed, as the claim numbers erroneously skipped from claim 6 to claim 8 due to typographical error; claim number 7 has been now used for a new dependent claim.

Claims 1–6 and 8–12 were rejected by the Examiner under 35 U.S.C. § 102 (b) as being anticipated by U.S. Patent No. 6,119,236 to *Shipley* (hereinafter *Shipley*).

Specifically, and in accordance with the interview with the examiner, independent claims 1, 6, 8, 10, and 11 have been amended to recite limitations directed to methods and systems for the analysis of network communication traffic for potential suspicious activity based on identified "flows." In general (e.g. claim 1 and others), these flows are derived by monitoring the exchange of packets between two hosts that are associated with a single service on the network. In another aspect (e.g. claim 8), a flow is determined by monitoring the exchange of packets between two Internet Protocol (IP) addresses wherein at least one port at one of the Internet Protocol addresses remains constant. Further aspects (e.g. dependent claims 13–16) relate to determining a flow based on predetermined characteristics, e.g. when no packets are exchanged between two hosts for a predetermined amount of time, a FIN flag, RESET packets, etc.

It is noted that the claim language has been changed from monitoring for potential "intrusion" activity to potential suspicious activity, so that it is clear that the activity need not be purely an external type activity, which the term "intrusion" might overly suggest. The application contemplates the danger of having an outside intruder gain control of an internal host (specification page 2, line 24), inspection of inbound and outbound activity and identifying suspicious patterns (specification page 4, line 26–27), determining if a flow appears to be legitimate traffic or possible suspicious activity (specification page 11,

line 20), etc. No limitation to external "intrusions" is intended, as there can be an "intrusion" to one host by another host inside a network .

Independent claim 12 is directed to detecting a particular type of suspicious activity that the present inventor has discovered, namely, that a plurality of UDP packets containing very little data (e.g. two bytes or less) may be indicative of a probe or potential intrusion.

Support for the present independent claim amendments can be found in the specification, among other places, at page 9, lines 8–27; page 18, lines 12–19; and page 19, lines 3–31. No new matter has been added by this amendment.

An indication of support for the various new dependent claims is recited specifically in detail below in a separate section.

35 U.S.C. § 102 (b) REJECTION UNDER *SHIPLEY*

Independent claims 1, 6, 8, 10, 11 and 12 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Shipley*. In view of the amendments to these claims, it is believed that the claims are not anticipated – without admitting that the claims were ever really anticipated. Accordingly, the amendments made herein are for clarity in understanding the claimed subject matter.

The *Shipley* patent relates to an intelligent network security device (INSD) that is configured to operate within a local area network ("LAN"), wherein the LAN is in communication with the Internet via a firewall. Within the internal boundaries of the firewall, the INSD monitors the LAN's communications that travel through the firewall looking for specific codes and patterns of behavior. (*Shipley*, Abstract.) The *Shipley* INSD assigns a value to any perceived attempted network security breach. Based upon the attempted security breach assigned value, the INSD instructs a firewall to take any of a prescribed plurality of actions.

As to the *Shipley* method of looking for "specific codes," it is apparent that such analysis requires inspection of data in each packet known to be indicative of security

breach attempts. (*Shipley*, col. 5, lines 60–62). This is clearly not a flow-based methodology.

As to the *Shipley* method of looking for "known patterns," this methodology is not clearly spelled out in the patent. These "patterns of activity" (*Shipley* col. 6, line 9–14) are only generally described; very few specific examples are given aside from the very general description of an "ordered attempt to access each machine on a network" (col. 6, lines 17–18), or "access ports which do not exist" (col. 6, lines 32–33), or "access a port which is ... not used" (col. 6, lines 40–43).

However, there is clearly no teaching of using a flow-based approach to detecting suspicious activity, and no specific analytical method described at all. Indeed, *Shipley* clearly asserts that "in order for the 'look for known patterns' operation 36 to be successful, the INSD 10 might require some knowledge of the configuration of the LAN 12 ..." (Col. 6, lines 57–60). This does not teach or suggest anything relating to use of a flow-based detection approach.

For the reasons that will be explained, the flow-based detection approach as recited in the claims of the present application is patentably different from the specific code- and pattern-based approach in the *Shipley* patent.

More specifically, *Shipley* initially describes the INSD as monitoring all Ethernet packets that are coming or going through the firewall in a "receive input" operation. Following the "receive input" operation, the INSD performs a "look for known code" operation and a "look for known pattern" operation. (*Shipley*, FIG. 2.) Within the "look for known code" operation, the INSD makes a comparison between the data that is contained within each Ethernet packet to data that is known to be indicative of security breach attempts.

As described in *Shipley*, the "look for known code" operation is performed simultaneously with the "look for known patterns" operation. In the "look for known patterns" operation, the INSD examines the patterns of activity of the communications on the LAN. This aspect is described within *Shipley* as requiring that the INSD retain

certain data for a limited amount of time in order to identify and examine the patterns of communicative activity within the LAN.

Following the completion of the "look for known patterns" operation and the "look for known code" operation, the INSD in *Shipley* performs an "assign weight to breach" and "react" operation, respectively. The specific function of the "assign weight to breach" operation is to provide a value that is based upon the average of various factors that are used to ascertain if there is a perceived attempted network security breach. If the system determines that there is an attempted network breach, then following the "assign weight to breach operation," the "react" operation is performed. In the "react" operation, the INSD sends a control signal to the firewall via a serial cable. The control signal directs the firewall to perform any of a number of prescribed actions that are based upon the value that has been determined in the "assign weight to breach" operation. (See e.g. *Shipley*, col. 7, lines 50–57)

In contrast to *Shipley*, the claims in this application (as amended, and in certain aspects) describe systems and methods for determining potential suspicious activity based on determining "flows," not on known codes, and not as regards known patterns in the way described in *Shipley*. As described amply in the specification, a flow (for some claims, e.g. claim 1) is identified by monitoring the exchange of packets between two hosts, and identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined characteristic. In a related aspect (e.g. claim 8), a flow is identified by monitoring the exchange of packets between two hosts each having a particular Internet Protocol (IP) address, and identifying a flow corresponding to a predetermined plurality of packets exchanged between a particular port of one of the hosts that remains constant during the plurality of packets. Such steps are not disclosed, taught, or suggested in *Shipley*.

According to another aspect, claim 1 further recites assigning a concern index value to an identified flow based upon a predetermined characteristic of the flow. The concern index is cumulated and associated with a host. According to yet another aspect,

claim 1 recites issuing an alarm signal in the event that the accumulated concern index for a host exceeds an alarm threshold value.

Shipley does not disclose, teach or suggest a method determining whether traffic is legitimate or potential suspicious activity involving monitoring packets exchanged between two hosts on the data communication network, and then identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined characteristic. Nor does *Shipley* disclose, teach or suggest accumulating concern index (CI) values on a host by host basis, as recited in various aspects of the presently claimed invention.

In *Shipley*, a decision to issue an alarm (or signal a firewall to block certain packets) is entirely based upon a value that has been assigned to a "breach" that can be based upon a singular event that can be associated with a "look for known code" operation and/or a "look for known pattern" operation. The "assign weight to breach" operation provides a value based upon the average of various factors that are used to ascertain if there is a perceived attempted network security breach. This bears no relation to the monitoring of packets and identifying a flow based on a predetermined plurality of packets that relate to a single service, and/or delimited by a predetermined event.

Claim 6, as amended, is directed among other things to the aspect of identifying a flow corresponding to a predetermined plurality of packets exchanged between two hosts, collecting flow data from packet headers of the packets in the identified flow, and based on collected flow data, assigning a concern index value to the flow based on a predetermined characteristic of the flow. *Shipley* also does not teach that abnormal network traffic can be detected by inspecting only the statistics of flows that are built up by inspecting only the packet headers of packets. This invention allows for a system to process approximately on an order of magnitude more packets per second, since less data per packet is captured in the input buffer (about 100 bytes per packet, whereas the average packet size is about 600 bytes). The computation required per packet header examined is far less than the string comparisons and searches done by a common signature-based INSD such as in *Shipley*.

Claim 8, as amended, is directed among other things to the aspect of monitoring the exchange of packets between two hosts each having a particular Internet Protocol (IP) address, identifying a flow corresponding to a predetermined plurality of packets exchanged between a particular port of one of the hosts that remains constant during the plurality of packets, collecting flow data from packet headers of the packets in the identified flow, and based on the collected flow data, assigning a concern index value to the flow. For the same reasons as discussed in connection with claim 6, it is submitted that *Shipley* does not disclose, teach, or suggest the aspect of monitoring packet exchange between two hosts each having a particular IP address, and identifying a flow based on a port remaining constant during a plurality of packets. (The aspect of the port remaining constant was recited in clam 8 as originally filed, and is supported in the specification on page 5, lines 11-12.)

Claim 10, as amended, is directed to a system that is operative to carry out flow-based detection of suspicious network activity. Claim 10 recites operations, along the lines of claim 1, wherein a computer system monitors the communication of packets on a data communication network and classifies the monitored packets into flows, wherein a flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network. For the same reasons as discussed above, it is submitted that *Shipley* does not disclose, teach, or suggest a system that operates as set forth in clam 10, as amended.

Claim 11, as amended, is also directed to a system that is operative to carry out flow-based detection of suspicious network activity. This claim recites the aspect where a processor monitors packets and classifies the monitored packets into flows, wherein a flow corresponds to a predetermined plurality of packets exchanged between two hosts that is associated with a single service on the network. In addition, claim 11 recites the aspects of maintaining a flow data structure, cumulating concern index values, and maintaining a host data structure for storing data associating a cumulated concern index value with each one of a plurality of hosts. For these reasons, as well as the reasons

discussed above, it is submitted that *Shipley* does not disclose, teach, or suggest a system that operates as set forth in claim 11, as amended.

Claim 12, as amended, is directed to a particular method of analyzing network communication traffic for potential suspicious activity involving a "short UDP," i.e. a plurality of datagrams having essentially no data, which the present inventor has discovered as indicative of a particular type of probe. As in other claims, this claim recites monitoring packets exchanged between two hosts on the data communication network. In addition, this claim recites identifying packets provided by one of the two hosts that have a transport level protocol specifying a packet format that includes a data segment. In response to determination that the transport level protocol is a User Datagram Protocol (UDP) packet and the data segment associated with the UDP packet contains two bytes or less of data, a concern index value of a predetermined amount is stored in a memory in association with information identifying the host that issued the UDP packet. Support for this claim is found in the specification on page 17, line 31 – page 18, line 5; original claim 12; and FIG. 7 ("short UDP"). It is submitted that neither the *Shipley* patent nor any other reference of record discloses, teaches, or suggests such a method.

Therefore, in view of the above remarks the Applicant respectfully request that the rejection under 35 U.S.C. § 102(b) of independent claims 1, 6, 8, 10, 11 and 12 be withdrawn.

THE DEPENDENT CLAIMS

New dependent claims 13–33 are presented for entry. These new dependent claims raise no new issues not already considered by the examiner, are supported in the specification (as will be shown), are not new matter, and are entered to provide additional protection for the claimed inventions especially as regards the doctrine of claim differentiation.

New dependent claims 13–16 qualify various independent claims and recite that the predetermined characteristic that identifies a flow can be elapse of a predetermined

time, a FIN flag, predetermined characteristics of traffic, and/or a RESET packet. Support is found in the specification on page 9, line 26 – page 10, line 7; and page 17, lines 1–8.

New dependent claim 17 qualifies the method of claim 1 and recites that the single service comprises a port number remaining constant for a plurality of packets. Support is found in the specification on page 5, lines 10–12.

New dependent claim 18 recites that the suspicious activity is from an inside address or from an outside address, to make it clear that the invention is not necessarily limited to detecting suspicious activity originating from external sources. Support is found in the specification on page 28, lines 17–26, which discusses the maintenance of host lists of "inside addresses" as well as "outside addresses."

New dependent claim 19 qualifies claim 1 by reciting that the concern index for a suspicious activity is derived by reference to a table of predetermined suspicious activities each having a predetermined concern index value. Support is found in the specification on page 17, line 15, and FIG. 6 and 7.

New dependent 20 qualifies claim 1 by reciting that the host for which the concern index is accumulated is an inside host. Support is found in the specification on page 28, line 24.

New dependent 21 qualifies claim 1 by reciting that the host for which the concern index is accumulated is an outside host. Support is found in the specification on page 28, line 24.

New dependent claim 22 qualifies claim 1 by reciting that the steps are carried out in a monitoring appliance. Support is found in the specification in FIG. 8 and the corresponding discussion on page 29.

New dependent claim 23 qualifies claim 22 by reciting that the monitoring appliance is installed behind a firewall. Support is found in the specification on page 12, line 12.

New dependent claim 24 qualifies claim 22 by reciting that the monitoring appliance is connected before a firewall. Support is found in the specification on page 12, line 11.

New dependent claim 25 qualifies claim 22 by reciting that the monitoring appliance is connected in a "DMZ". Support is found in the specification on page 12, line 14.

New dependent claim 26 qualifies claim 22 by reciting that the monitoring appliance is configured to operate as a pass-by filter. Support is found in the specification on page 29, line 17.

New dependent claim 27 qualifies claim 22 by reciting that the monitoring appliance is coupled to a network device. Support is found in the specification on page 12, line 6, and in FIG. 8.

New dependent claim 28 qualifies claim 27 by reciting that the network device is selected from group comprising a router, switch, hub, and/or tap. Support is found in the specification on page 28, line 18.

New dependent claim 29 qualifies claim 27 by reciting that the network device is a network security device. Support is found in the specification on page 29, line 10.

New dependent claim 30 qualifies claim 1 by reciting that the monitoring of packets comprises monitoring on packet header information only. Support is found in the specification on page 15, line 18, and other places that describe the packet header processing.

New dependent claim 31 qualifies claim 1 by reciting that the monitoring of packets is carried out in a device operating in a promiscuous mode. Support is found in the specification on page 29, line 26.

New dependent clam 32 qualifies claim 1 by reciting that the alarm signal is provided to a utilization component. Support is found in the specification on page 29, lines 1–11, and page 34 lines 1–8.

New dependent claim 33 qualifies claim 32 by reciting various types of utilization components, with support found in the same places as for claim 32. Such components

include, for example, network security devices, email, SNMP trap message, beeper, cellphone, firewall, network monitor, and user interface display to an operator.

Finally, for the record, this substitute amendment is submitted in place of the document timely filed on January 17, 2006, so that claim language relating to the manner of identifying a flow would not be interpreted as requiring that a flow "terminate" or be "delimited" before it is identified. This substitute amendment changes certain language in claim 1 and in certain dependent claims to recited that flow may be identified, among other things, as "characterized by a predetermined characteristic." This change was necessary because it is not believed that the invention is limited to identifying a flow only when it is terminated or delimited. No new matter is added; the only change relates to ensuring that the claims are not interpreted in an unduly narrow manner as regards this issue.

* * * * *

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed September 15, 2005 and is believed to place all claims in the application in condition for allowance. Accordingly, it is respectfully submitted that this application be allowed and that a Notice of Allowance be issued. If the Examiner believes that a telephone conference with the Applicant's attorneys would be advantageous to the disposition of this case then the Examiner is encouraged to telephone the undersigned.